Sandy Bacik

From: Sandy Bacik
Sent: Friday, March 09, 2012 11:18 AM
To: csctgarchi@nist.gov
Subject: CSWG Architecture minutes from 20120308

CSWG Architecture twiki: http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/CsCTGArchi
Chair: Elizabeth Sisley (sisley@cs.umn.edu)

20120308 Minutes

1. Current Tasks.
    a. To catch everyone up on our consensus work, a summary pdf of the conceptual security architecture work can be found here: https://collaborate.nist.gov/twiki-sggrid/pub/SmartGrid/CsCTGArchi/Conceptual_Security_Architecture_-_Consensus_Progress.pdf.
    b. Our current services spreadsheet is here: https://collaborate.nist.gov/twiki-sggrid/pub/SmartGrid/CsCTGArchi/Security_Services-And-MessageList-v0p6.xls.
    c. Using our power point (http://collaborate.nist.gov/twiki-sggrid/pub/SmartGrid/CsCTGArchi/20120216-SecurityServicesToMessages.ppt) we started to reviewing services mapping to messages for messages that did not map to every security service.
        i. We had consensus on the call to combine all of the Authentication security services into a single authentication service and apply it across the Smart Grid enterprise, components, and applications, and all message types.
        ii. We had consensus in the conceptual security architecture to ensure there is a requirement to use secure network time protocol for all messages.
    d. This is Sandy's rationalization for the last 20 services and mapping to message types.
        i. A message is an interaction between two actors using a specific security service - an exchange of information.
        ii. Our messages are generic to align with the SGAC conceptual architecture interaction definitions.
        iii. When we select a security service for a message type, this means that every time the message type is used the utility shall implement and apply the security service. We are NOT specifying any specific technology to use for the security service, just what security service shall be implemented.
        iv. Authentication service should be applied to all message types to ensure that the messages are coming from a valid source.
        v. Availability / Reliability (Managing the operational capability of smart grid assets to ensure they are operational when accessed). The availability / reliability security service needs to be applied to the following message types, because these message types need to be operational during any event or situation: acknowledgement, alarm, alert, command, error, identification, notification, query, response, schedule, setting, time, and work order.
            1. NOTE: We may want to consider, to simplify the services, combining the availability / reliability, contingency planning, crisis management, disaster recovery, incident response, and incident reporting into few security services with more generic definitions to lessen confusion.
        vi. Confidentiality - message contents security service needs to always be applied to these message types: command, identification, setting, and time. Optionally, a utility may add additional message types depending upon the operation.
            1. NOTE: We may want to consider, to simplify the services, combining confidentiality - message contents, confidentiality - stored data, and confidentiality - traffic flow. Although transmission confidentiality may be required for a message, but when it is stored in the back office it may not need to remain confidential.
        vii. Confidentiality - stored data security service needs to always be applied to these message types: contract, policies, and settings

viii. Confidentiality - traffic flow security service needs to always be applied to these message types: alarm, alert, command, identification, response, setting, and usage information

ix. Contingency Planning security services needs to always be applied to these message types: alarm, alert, command, identification, schedule, and time, because these message types need to have alternate routes to the operations center and need to be available during an event.

x. Crisis Management security service needs to always be applied to these message types: command, contract, forecast, plan, schedule, setting, because these are the message types that operators would need to keep operational.

xi. Directory Service security service needs to always be applied to these message types: none, because none of the message information or structure should be stored within a directory service or LDAP.

xii. Disaster Recovery security service needs to always be applied to these message types: alarm, alert, command, error, identification, resources, schedule, setting, time, because during an event an operator needs to have access to these types of messages to make operational decisions.

xiii. Integrity Protection - Hardware security service needs to always be applied to these message types to ensure that hardware is not altered during implementation or operation: acknowledgement, alarm, alert, command, error, identification, notification, query, response, schedule, setting, status, time, usage information - this means that the logs stored locally need to have hardware to protect to ensure the hardware tampering does not impact the logs.

    1. NOTE: We may want to consider, to simplify the services, combining integrity protection - hardware, integrity protection - software, and integrity protection - stored data, and integrity protection - message and state that all interactions need to have integrity for communication of information.

xiv. Integrity Protection - Software security service needs to always be applied to these message types to ensure that the underlying software is protected: contract, plan, policies, product, and work order - many of these are more business artifact than an actual interaction.

xv. Intrusion Detection security service needs to always be applied to these message types to ensure that anomalous events or replay or some incident can be identified: acknowledgement, alarm, alert, audit, command, error, identification, notification, query, response, schedule, setting, status, and time.

xvi. Physical Security security service needs to always be applied to these message types: forecast, plan, product, and work order.

xvii. Security Alarm Management security service needs to always be applied to these message types to interact with incident response or crisis management type services: alarm, alert, command, error, identification, setting, and time.

xviii. Security Measurement and Metrics security service needs to always be applied to these message types to interact with incident response or crisis management type services to produce metric to support operations: alarm, alert, audit, command, error, identification, setting, status, and time.

xix. Security Monitoring security service needs to always be applied to these message types to interact with incident response or crisis management type services: alarm, alert, audit, command, error, identification, notification, query, response, schedule, setting, status, and time. These messages would interact with an SEIM.

xx. Security Operations Management security service needs to always be applied to these message types to assist in the operational monitoring: alarm, alert, audit, command, error, identification, notification, query, response, schedule, setting, status, and time.

xxi. Security Policy Management security service needs to always be applied to these message type to ensure that operators and engineers are complying with policy: policies, resources, and work order.

xxii. Security Training and Awareness security service needs to always be applied to these message types to ensure that operators know how to use and response to the messages: forecast, plan, policies, product, and work order.

    1. NOTE: we may want to make this an enterprise level security service and all types of information needs to be included in the security training and awareness programs.

xxiii. Software Licensing security service needs to always be applied to these message types to ensure that licensing agreements are not violated: forecast, plan, policies, product, schedule, and work order.

xxiv. System Configuration Protection security service needs to always be applied to these message types to ensure configuration protection: command, contract, forecast, identification, resources, schedule, setting, status, and time.

1. NOTE: Or by applying this at the enterprise, component, and application levels, this implies that the message types do not need a separate configuration protection.

xxv. User Interface for Security security service, is a different one, because this focuses on an application not presenting obstacles or unclear explanation of key message types for users to be able to respond to: forecast, plan, policies, product, resources, schedule, setting, and work order.

xxvi. User Support security service is to manage operational user issues related to security and needs to always be applied to these message types: command, contract, forecast, plan, policies, product, resources, schedule, and work order.

xxvii. NOTE: The security services and message types should be reviewed for their definitions to ensure they are generic and broad enough to allow a utility to use in their environment without specifying a technology that will be required.

xxviii. NOTE: In reviewing and understanding the security services, if they can be combined to make the conceptual more abstract, then the definition can be updated and the security services be combined.

2. Open Items.
   a. We said good bye to Sandy Bacik.
   b. Please help Elizabeth move forward with our updates to the NISTIR 7628 chapter 2.
   c. We need to more volunteers to participate during our calls.
3. Attendees.
   a. Dan Friedman
   b. Elizabeth Sisley
   c. Marianne Swanson
   d. Neil Greenfield
   e. Sandy Bacik
   f. Stephen Chasko

Regards,
Sandy Bacik, CISSP, CISM, ISSMP, CGEIT
Principal Consultant
EnerNeX
p: 865.696.4470
e: sandy.bacik@enernex.com // www.enernex.com